UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
---X

STONEX GROUP, INC. et al.,

Plaintiffs,

-against-

HOWARD SHIPMAN,

Defendant.
---X

23-CV-00613 (JGK) (VF)

REPORT & RECOMMENDATION

VALERIE FIGUEREDO, United States Magistrate Judge

TO: THE HONORABLE JOHN G. KOELTL, United States District Judge.

By motion dated June 20, 2023, Plaintiffs StoneX Group Inc. and StoneX Financial Inc. (collectively, "StoneX") seek spoliation sanctions pursuant to Federal Rule of Civil Procedure 37(e) against Defendant Howard Shipman, including terminating sanctions, for his failure to preserve electronically stored information ("ESI"). See ECF No. 106. For the reasons that follow, I recommend that StoneX's motion for sanctions be **GRANTED**. Specifically, I recommend that default judgment be entered against Shipman as to the claims asserted by Plaintiffs in their complaint; that an order striking the counterclaims asserted by Shipman be entered; and that monetary sanctions be awarded to Plaintiffs for the attorneys' fees and costs incurred in bringing the motion for spoliation.

BACKGROUND

A. Factual Background[1]

1. Shipman's employment with StoneX

StoneX Group Inc. is a publicly traded financial services organization. See ECF No. 30 ("Compl.") ¶¶ 2, 8. StoneX Financial Inc. is StoneX Group Inc.'s broker-dealer entity. Id. ¶¶ 3, 9. StoneX hired Shipman in February 2021 to be co-head of Quantitative Strategies at StoneX Financial. Id. ¶¶ 4, 10, 14-15, 18. StoneX gave Shipman a company-owned laptop for his use in performing work for StoneX. Id. ¶¶ 20, 27. The Quant Group, of which Shipman was a part, was tasked with developing "new capabilities" for StoneX, including an internally developed and confidential electronic-market-making software named Project Pascal. Id. ¶¶ 15-17, 53, 59-68.

Shipman was the developer of certain aspects of this confidential and proprietary software for StoneX. Id. ¶¶ 53-57, 68. For example, Shipman was the developer of "Texas," which is one of the "three main code libraries" comprising the code for Project Pascal. Id. ¶¶ 54, 57. StoneX stores the code for Project Pascal in a code "repository," which is an archive of computer source code stored on servers. Id. ¶ 55. Following Project Pascal, StoneX began development of Darwin, and the computer code for Darwin was written and stored on StoneX Pascal Azure servers. Id. ¶¶ 59-62. On December 9, 2022, prior to his termination that day, Shipman provided a virtual presentation concerning Darwin to the then-current Quant Team. Id. ¶ 68. In that presentation, Shipman presented portions of Darwin source code, among other things. Id.

[1] Unless otherwise noted, citations to documents filed on the electronic docket ("ECF") are to the original pagination in those documents.

Later on December 9, StoneX terminated Shipman's employment. Id. ¶¶ 10, 15, 71-73. By December 12, 2022, Shipman had retained counsel and Shipman's counsel had contacted StoneX to discuss potential employment-related claims by Shipman against StoneX. See ECF No. 130 ("Tr.") at 24-25 ; see also ECF No. 108-3; ECF No. 108-4 at 1.

2. The instant lawsuit

On December 27, 2022, StoneX sent a letter to Shipman's counsel, informing counsel that StoneX was considering filing claims against Shipman for misappropriation of StoneX's confidential information and trade secrets. See ECF No. 108-4 at 1. In the letter, counsel for StoneX noted that Shipman's counsel had previously indicated that Shipman had "various employment-related claims against StoneX." Id. The letter instructs counsel of Shipman's obligation to preserve documents and records "that may be relevant to" both Shipman's claims against StoneX and Stone's claims against Shipman, including, for example, "all copies in whatever form of the project Darwin code, the Project Pascal Code, or any code developed since the beginning of your Employment with StoneX." Id. at 1-2. The letter further asked Shipman to preserve, among other things, "all personal electronic devices," including USB drives and "all infrastructure and services purchased and hosted in Akami's Linode Cloud Computing." Id. at 2-3.

On January 24, 2023, StoneX commenced this action against Shipman, asserting claims for violation of the Defend Trade Secrets Act, 18 U.S.C. § 1839, violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, misappropriation of trade secrets, breach of fiduciary duty, and conversion. Compl. ¶¶ 119-53. The complaint alleges that Shipman, after his termination and without authorization, logged into StoneX servers and executed an "unknown number of commands, deletions, and/or other actions," including extracting 87 megabytes of data from StoneX's server. Id. at ¶¶ 75-89. StoneX seeks permanent injunctive relief. Id. ¶¶ 7, 127, 135, 139, 147.

On January 26, 2023, Shipman signed a "voluntary stipulation," which the Honorable John G. Koeltl signed and entered that same day. See ECF No. 16. In that stipulation, Shipman agreed to, among other things, "account for any and all of StoneX's proprietary, confidential and/or trade secret information currently in [his] custody or control" and grant Charles River Associates ("CRA") access to computers and electronic devices in his home for purposes of CRA examining those devices and removing copies of StoneX's proprietary information. Id. On February 10, 2023, Judge Koeltl entered an order instructing Shipman to "take any necessary steps to ensure that evidence is not destroyed, even by routine data destruction protocols by third parties." See Feb. 10, 2023 Order, filed under seal. On February 28, 2023, Judge Koeltl signed and entered the parties' joint proposed forensic review protocol. See ECF Nos. 45, 51 (forensic review protocol filed under seal). The forensic review protocol addressed how Shipman's privileged and otherwise confidential information, such as the medical records of his children and spouse, would be excluded from CRA's forensic review of Shipman's electronic devices. See ECF No. 51 at ¶ 8.

3. *The forensic examination of StoneX's systems and Shipman's electronic devices*

After Shipman's termination, StoneX retained CRA to perform a forensic examination of StoneX's systems and Shipman's electronic devices. Compl. ¶¶ 90-91; see also ECF No. 108-1, Expert Report of R. Cuyler Robinson ("Robinson Report") ¶¶ 6-7, 29. Beginning on December 27, 2022, CRA conducted a collection and analysis of information and forensic evidence from

StoneX, including evidence from StoneX computers, servers, and systems used by Shipman. Robinson Report ¶ 20. Additionally, CRA also collected and examined Shipman's home computers, devices, and accounts. Id. ¶ 108. The collection of Shipman's personal computers and devices occurred on March 2, 2023. Id. ¶ 23. R. Cuyler Robinson of CRA prepared an expert report dated May 16, 2023. Id. In that report, Robinson made the following findings and reached the following conclusions.

CRA examined a copy of a StoneX virtual computer, named Corvo-004, that was used by Shipman to develop and test StoneX source code. Id. ¶ 70. To access StoneX's virtual computers, Shipman used a user account named "pianoman." Id. ¶ 72. On December 9, 2022, 87 megabytes ("MB") were transferred from the Corvo-004 server, and as that transfer was occurring, the "bash history log files and other data" were deleted from the server. Id. ¶ 73; see also Compl. ¶ 83. A log file is a record of historical events that occurred on a computer. Robinson Report ¶ 67. A bash history is a log file created on computers with a Linux operating system. Id. ¶ 68. By default, a bash history stores the last 500 commands that a user has executed from the Linux operating system interface. Id. ¶ 69. Deleting the bash history log file destroys the record of previously issued commands and "obfuscates" the activities that occurred in the Linux environment. Id. CRA's inspection determined that the bash history log file for the "pianoman" account on StoneX's Corvo-004 server was deleted. Id. ¶ 75. Additionally, the bash history log file for the root account on the Corvo-004 server was also deleted on December 9. Id. ¶ 76. The root account is the "default and primary administrator account" on Linux computers. Id. As Robinson explains, Shipman had access to, and used, the root account on the Corvo-004 server. Id.

CRA also determined that on December 9, 2022, four files of Darwin source code were accessed and deleted from the Corvo-004 server. Id. ¶¶ 78-87. CRA confirmed which Darwin source code files existed on December 9 within a "projects" folder on the Corvo-004 server; those files were "accessed" on December 9; and although the four Darwin source code files should have contained a "projects folder," the project folders did not exist. Id. ¶¶ 78-83. Robinson opined that the StoneX source code files and the project folders accessed on December 9 were deleted likely on that day. Id. ¶ 83. In addition to the accessed files, the user folders for the "pianoman" account, including "Desktop, Downloads, and Documents," were also deleted, along with the bash history log file. Id. ¶¶ 84-87.

On December 10, 2022, a "SanDisk Cruzer" USB drive was connected to Shipman's StoneX laptop. Id. ¶ 47. On December 14, 2022, the same SanDisk Cruzer USB drive was again connected to Shipman's StoneX laptop and 16 folders were created on the SanDisk USB drive "in succession and within seconds of each other." Id. ¶¶ 47-49. The 16 folders were created within a folder tiled "StoneX Docs." Id. ¶ 48. Based on his experience, Robinson explained that the activity was consistent with copying folders and files from the StoneX laptop to the USB drive. Id. ¶¶ 50-51. Robinson was also able to determine that 13 of the 16 folders copied from the laptop to the USB drive contained "StoneX branded and confidential information." Id. ¶ 50. The remaining three folders (and any files contained within them) that were copied to the USB drive were deleted from the laptop. Id. One of those folders was titled "StoneX Docs\Texas" and another was titled "StoneX Docs\Darwin." Id. There were no source code files within the "Darwin" folder on the StoneX Laptop and the "Texas" folder had been deleted from the laptop and was not recoverable. Id. On December 19, 2022, the same SanDisk Cruzer USB drive was connected to Shipman's personal desktop computer. Id. ¶¶ 118, 158. Shipman gave the SanDisk Cruzer USB drive to CRA for forensic examination, but the drive was non-functional due to physical damage. Id. ¶¶ 118, 125, 158-61. Although the drive was non-functional, CRA determined that the data on the drive was removed or destroyed before any physical damage had occurred. Id. ¶¶ 159-60.

On December 14, 2022, a "VirtualBox" folder and the files it contained were deleted from Shipman's StoneX laptop.[2] Id. ¶ 52. As of December 14, a virtual box named "deckard" existed on Shipman's StoneX laptop, but the virtual box and any files contained within it were deleted on December 14. Id. ¶¶ 53-54. Robinson explained that the deletion of "deckard" was like "destroying an entire computer and its storage drive."[3] Id. ¶ 54. Moreover, the deletion of "deckard" prevented CRA from conducting a forensic examination of the virtual box. Id. CRA was able to determine that on December 14, the SanDisk Cruzer USB drive had been connected to the StoneX laptop when the virtual box was deleted from the laptop, and the USB drive was disconnected one minute and 13 seconds after the virtual box had been deleted. Id. ¶ 55. In Robinson's opinion, this indicated that "Shipman may have transferred the files from the VirtualBox folder" to the SanDisk Cruzer USB Drive and then deleted the virtual box from the laptop. Id.

[2] VirtualBox, a virtualization software developed by Oracle, is used to create and operate "virtual machines," which are virtualized computers that can be created, saved, and run on "host" computers. Robinson Report n.17.

[3] Robinson also concluded that Shipman "created and accessed multiple virtual machines" using his personal desktop computer and that he had "deleted at least one, possibly two, virtual machines" from his desktop computer. Robinson Report ¶ 119.

On December 17, 2022, a SanDisk "SSD" drive was connected to Shipman's personal desktop computer. Id. ¶ 110. Shipman did not provide this SanDisk drive to CRA, despite being obligated to do so pursuant to the Court's January 26, 2023 order. Id. ¶¶ 110, 174.

On December 19, 2022, 10 days after Shipman's termination, the system clock of Shipman's StoneX laptop computer was temporarily altered. Robinson Report ¶¶ 34-36. The Microsoft Windows systems event log showed that the system date on the StoneX laptop used by Shipman was manually backdated to December 5, 2022, for approximately 37 minutes, after which time the date was changed back to the correct date of December 19. Id. ¶¶ 34-35. CRA determined that during the period of time when the system date on the laptop was altered, a Sony USB drive was connected to the StoneX laptop and at least 256 StoneX source code files were copied using Robocopy, a file copying program that can preserve timestamp and metadata of the files and folders it copies. Id. ¶¶ 37-42, n.11. The files were copied from a folder on the StoneX laptop titled "research" to a folder on the Sony USB Drive. Id. ¶¶ 40-42. The folders containing the source code files that had been copied to the laptop were deleted from the StoneX laptop before CRA's inspection of the laptop. Id. ¶ 43. Robinson opined that Shipman used Robocopy and altered the laptop's clock in order to hide the actual date the files were copied and to preserve the backdated timestamps for those files. Id. ¶¶ 15, 46. Pursuant to the Court's January 26 order, Shipman was obligated to provide the Sony USB drive used on December 19 to CRA. Shipman failed to do so, stating in his declaration that the device's location was unknown. Robinson Report ¶¶ 59, 175. Without the Sony USB drive, Robinson was unable to recover information directly from the device, including the missing StoneX source code files that had been copied to it. Robinson Report ¶¶ 57-59.

On December 19, the same Sony USB Drive which had been connected to Shipman's StoneX laptop on that day was also connected to Shipman's personal desktop computer. Id. ¶¶ 109-112. CRA determined that on December 19, the StoneX source code files that were copied using the StoneX Laptop and Sony USB Drive were also copied to Shipman's desktop computer. Id. ¶¶ 113-16. Some of the folders that were copied were titled "research" and "research\durango." Id. ¶ 114. Durango is a "predecessor to Darwin" source code. See ECF No. 108-2 (573:5-9). On March 2, when CRA forensically imaged Shipman's desktop computer, the folder and any of the StoneX source code files contained in those folders no longer existed on the computer, "indicating that they had been deleted (and potentially wiped using a file wiping program)." Id. ¶¶ 113-17.

On December 20, 2022, a TOR web browser was installed on Shipman's personal desktop computer. Id. ¶ 150. TOR is a web browser that anonymizes web traffic and, unlike other web browsers, TOR does not store web browser history by default. Id. ¶ 151. TOR was used "multiple" times between January 4, 2023, and February 6, 2023, on Shipman's desktop computer. Id. at ¶ 150. CRA determined that the program files for TOR were deleted "at some point after February 6, 2023, the last time TOR was used." Id.

On December 21, 2022, BitWipe, "a commercial file wiping program that has a free trial period," was used on Shipman's personal desktop computer. Id. ¶ 128. That same day, Eraser, "a free file wiping tool," was also used on Shipman's desktop computer. Id. ¶ 129.

On December 26, 2022, the file wiping program SDelete was used on Shipman's StoneX laptop. Id. ¶¶ 60-62. CRA determined that on December 26, 2022, within a "temporary folder under the howard.shipman user profile" on the laptop, 967 unique "SDELMFT" files were created. Id. ¶ 63. As Robinson explains, "SDELMFT" files are automatically created by SDelete as part of the file wiping process, which indicated that SDelete had been used to "destroy data" on Shipman's StoneX laptop. Id. ¶¶ 62-63. CRA determined that the SDelete file wiping program was stored on a Memorex USB storage drive, but that drive was not produced to CRA despite Shipman being required to do so.[4] Id. ¶¶ 120-23.

Additionally, on December 26, 2022, Shipman downloaded, installed, and used SDelete on his personal desktop computer. Id. ¶ 130. Between December 26 and March 2, 2023 (just hours before CRA was scheduled to forensically image Shipman's computers), SDelete was used 94 times. Id. On February 2, 2023, Shipman created a "script" that was used at least 79 times to execute the SDelete file wiping program on his personal desktop computer. Id. ¶¶ 134-36. Robinson determined that one file that was deleted using SDelete was a file related to the "Tampa" source code—a source code that was part of StoneX's Project Pascal. Id. ¶ 136; see also Compl. ¶¶ 53-54. Additionally, Robinson determined that on February 2, 2023, Shipman created a "script file" named "sys.dat" that was used to hide the execution of SDelete on the desktop computer. Robinson Report ¶¶ 134-35, 188. Using SDelete, Shipman erased the "USB device connection information" from his personal desktop computer at some point between February 2, 2023, and February 22, 2023, "destroy[ing] some USB device connection information." Id. ¶¶ 126-27. Robinson concluded that Shipman had "used multiple file wiping

[4] The Memorex USB storage drive was first connected to Shipman's personal desktop computer on February 1, 2023, and last connected on February 15, 2023. Robinson Report ¶ 121. A second Memorex USB storage drive was connected to Shipman's desktop computer on February 28, 2023. Id. ¶ 122. This drive was produced by Shipman, but it contained video game files that were copied to the drive on February 28. Id.

programs, dozens of times, until the day CRA arrived at his residence to image his computers and devices." Id. ¶ 141.

Robinson's examination also revealed that the bash history log file on Shipman's personal desktop had been deleted. Id. ¶ 132. That bash history log contained commands previously used on the desktop computer between February 1, 2023, to March 2, 2023. Id. The bash history log file on Shipman's desktop computer had a "creation date of March 2, 2023," and contained only four previously issued commands. Id. Robinson was able to recover the deleted bash history log file, from February 1, 2023, to March 2, 2023. Id. ¶ 133. Through a review of that log, Robinson identified "anti-forensic and file wiping activity," such as the creation of a "script" file that was used 79 times to execute the SDelete file wiping program on the desktop computer. Id. ¶¶ 133, 136. Additionally, Robinson uncovered other commands in the bash history log file from Shipman's desktop computer that "were indicative of steganography," which is "the hiding of files or data within existing files or data." Id. ¶ 138. Robinson opined that "data, such as source code," may have been hidden within Shipman's "gaming and personal files," but he was unable to confirm if this had happened because the relevant files were deleted with SDelete and thus were unavailable. Id. Robinson determined that SDelete had been used to wipe "specific fantasy gaming files out of thousands of other fantasy gaming files" on Shipman's desktop computer. Id. ¶ 140. Robinson opined that "deleting seemingly irrelevant files that could have been packed with other data . . . is consistent with hiding evidence of a steganography technique." Id.

CRA obtained access to Shipman's Linode computer on March 2, 2023. Id. ¶¶ 93-94. Linode is a cloud hosting provider that offers inexpensive virtual computer hosting services. Id.

¶ 88. At that time, there was only one Linode computer available for review, named "Sovngarde," and it had been created on February 24, 2023. Id. ¶ 95. CRA's forensic examination determined that a Linode computer belonging to Shipman was used to connect 532 times to eight StoneX computers between December 7, 2021, and December 9, 2022. Id. ¶¶ 89-91. By the time Robinson was given access to Shipman's Linode account, three Linode computers on Shipman's account had been permanently deleted, could not be recovered, and could not be forensically examined. Id. ¶¶ 94, 98-99, 101. The three Linode computers were deleted on December 13, 2022, December 14, 2022, and December 15, 2022. Id. ¶¶ 98.

CRA also discovered that between February 2, 2023, and March 2, 2023 (the day CRA collected forensic evidence from Shipman's home), Shipman created and referenced a file on his desktop computer titled "xf." Id. ¶ 142. The "xf" file contained a list of numerous system "artifacts" that are commonly examined during a forensic investigation and was "essentially an anti-forensics 'playbook' of system artifact locations." Id. One of those forensic artifact locations is a computer's ShimCache and Background Activity Monitor ("BAM"). Id. ¶ 145. As Robinson explains, if system artifacts are deleted or altered by a user, it would inhibit a complete understanding of the past events that occurred on a computer. Id. ¶ 143. The xf file on Shipman's desktop computer was opened at least nine times between February 2, 2023, and March 2, 2023, and although the file was deleted from Shipman's computer on March 2, 2023, CRA was able to recover it. Id. ¶¶ 142, 144. Robinson opined that creating and referencing the xf file was an "attempt to obfuscate activities on" Shipman's desktop computer. Id. ¶ 149. Additionally, the ShimCache and BAM on Shipman's desktop did not contain any entries for the SDelete file wiping program, even though the program had been executed at least 94 times, suggesting to Robinson that the entries had been deleted. Id. ¶¶ 142-46.

CRA determined that at least nine USB storage drives were connected to Shipman's StoneX and personal computers. Id. ¶ 165. Of those drives, four were provided to CRA for inspection. Id. ¶ 170. Of the four drives, two had personal data (such as video game data) that had been copied to them on February 28, 2023, two days before CRA was scheduled to collect forensic evidence. Id. Robinson explained that if previously existing data is overwritten when new data is copied to the drive, then the previously existing data would not be recoverable through a forensic analysis. Id. ¶ 168. According to Robinson, the copying of personal data so close in time to CRA's inspection suggested that irrelevant data was copied to the storage drives to "potentially overwrite existing data on the USB storage drives." Id. ¶ 170.

On March 2, 2023, CRA also inspected Shipman's personal laptop computer. Id. ¶ 152. CRA analyzed the laptop and concluded that it had been overwritten. Id. ¶¶ 154, 157. There were no operating system files, user files, or other file data that would indicate an operating system was installed on the laptop. Id. ¶ 154. Robinson explained that Shipman provided a non-functional, "wiped" laptop to CRA for inspection. Id. ¶ 188.

Ultimately, Robinson opined that Shipman had engaged in extensive "anti-forensic efforts" in an attempt to destroy, alter, and hide relevant evidence using tools and techniques designed to alter or destroy data. Id. ¶ 13. Robinson further opined that Shipman's destruction and alteration of evidence impacted CRA's ability to identify the StoneX source code that Shipman accessed, copied, or deleted. Id. ¶ 14. Additionally, Robinson explained that he had identified certain StoneX data that had previously existed on StoneX computers, Shipman's personal computer, or Shipman's other devices but was never produced to CRA for forensic inspection. Id. ¶ 16.

4. Shipman's relevant testimony

StoneX's counsel deposed Shipman on two occasions. During his deposition on March 23, 2023, Shipman was asked by counsel if he had "run a wiping program" on his StoneX laptop or personal desktop computer. See ECF No. 108-8 at 151. Shipman responded "[n]o" and said that he did not "recall any wiping program," adding that he "didn't do it deliberately." Id. Shipman was also asked if he had run the SDelete file wiping program on his personal desktop computer. Id. at 187. Shipman testified that he could "recall no instances of downloading or running . . . this program on that computer." Id. Additionally, Shipman was asked if he recalled downloading a file named "xf" and then deleting it. Id. at 191. Shipman testified, "[n]o. Id.

Shipman was deposed again on June 14, 2023. See ECF No. 108-2. During the deposition, Shipman was asked whether it was possible that he "ran SDelete approximately 94 times" on his computer. Id. at 629. Shipman testified that he did not "recall executing SDelete" on his personal desktop computer. Id. at 629-31.

In a January 27, 2023 declaration submitted by Shipman, Shipman provided an explanation for what transpired on the Corvo-004 server on December 9, 2022. Under penalty of perjury, Shipman explained that he decided that the Corvo-004 server was the "best candidate to retire" and thus he ran "a series of scripts and background commands" to "sanitize or remove sensitive data" before its retirement. Declaration of Howard Shipman, dated January 27, 2023, filed under seal ("Shipman Decl.") ¶¶ 15-17. Robinson reviewed Shipman's declaration and opined that Shipman's "decision to retire the Corvo-004 Server [did] not make sense." Robinson Report ¶ 105.

5. *The instant motion*

On June 20, 2023, StoneX filed the instant motion for sanctions. See ECF No. 106. StoneX contends that Shipman intentionally destroyed ESI evidence, despite being under an obligation to preserve that evidence, in order to cover up his theft of StoneX's proprietary and confidential computer source code. See ECF No. 107 ("Pl.'s Br.") at 1-11. StoneX argues that Shipman's intentional destruction of ESI constitutes spoliation of evidence under Federal Rule of Civil Procedure 37(e), and it seeks terminating sanctions, in the form of an order striking Shipman's pleadings and precluding Shipman from putting forth any defense to StoneX's claims in this matter. Id. at 16-18, 26-30. In effect, StoneX seeks the entry of a default judgment against Shipman. See Tr. at 6. StoneX also requests monetary sanctions, in the amount of "all costs and expenses incurred by [StoneX] as a result of [Shipman's] deliberate acts of spoliation." Pl.'s Br. at 30-31.

Shipman, who was initially represented by counsel in this action, has been proceeding pro se since his counsel withdrew on May 25, 2023. See ECF Nos. 89, 91. On October 19, 2023, Shipman, proceeding pro se, filed an opposition to StoneX's motion. See ECF Nos. 120-21. StoneX filed a reply brief on October 26, 2023. See ECF No. 122. On January 3, 2024, Shipman submitted a supplemental memorandum in further support of his opposition to StoneX's motion. See ECF No. 125. I held oral argument on the motion on January 18, 2024. See ECF No. 130. On January 29, 2024, Shipman filed a supplemental submission. See ECF No. 132.

DISCUSSION

A. Legal Standards

"Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999). Federal Rule of Civil Procedure 37(e) governs sanctions for failure to preserve ESI. "If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery," the court:

> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> > (A) presume that the lost information was unfavorable to the party;
> >
> > (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
> >
> > (C) dismiss the action or enter a default judgment.

Fed. R. Civ. P. 37(e).

Under Rule 37(e), a court must first determine "if a party failed to take 'reasonable steps' to preserve electronically stored information 'that should have been preserved in the anticipation or conduct of litigation.'" Charlestown Cap. Advisors, LLC v. Acero Junction, Inc., 337 F.R.D. 47, 59 (S.D.N.Y. 2020) (quoting Fed. R. Civ. P. 37(e)). If so, two categories of sanctions are contemplated under the rule. Under Rule 37(e)(1), upon a showing of prejudice, the court "may order measures no greater than necessary to cure the prejudice." Fed. R. Civ. P. 37(e)(1); see also

Charlestown Cap. Advisors, 337 F.R.D. at 60. Sanctions under this subsection may include "forbidding the party that failed to preserve information from putting on certain evidence, permitting the parties to present evidence and argument to the jury regarding the loss of information, or giving the jury instructions to assist in its evaluation of such evidence or argument." Lokai Holdings LLC v. Twin Tiger USA LLC, No. 15-CV-9363 (ALC) (DF), 2018 WL 1512055, at *7 (S.D.N.Y. Mar. 12, 2018) (quoting Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment).

The second category of potential sanctions, under subsection (e)(2), "are particularly harsh," Lokai Holdings, 2018 WL 1512055, at *8, and, as the advisory committee's notes warn, "[c]ourts should exercise caution" in using them. Fed. R. Civ. P. 37(e) (advisory committee's note to 2015 amendment). Sanctions under this subsection may include "mandatory presumptions or instructions that the lost information was unfavorable or the entry of default judgment." Charlestown Cap. Advisors, 337 F.R.D. at 59. To award sanctions under subsection (e)(2), a court must "find that the party to be sanctioned acted with an intent to deprive," Charlestown Cap. Advisors, 337 F.R.D. at 60 (internal quotation marks omitted), but, unlike under subsection (e)(1), there is no requirement that a court find prejudice to the party deprived of the spoliated information, Lokai Holdings, 2018 WL 1512055, at *8. Although the rule is silent as to the standard by which the "intent to deprive" must be established, given the severity of the sanctions sought by StoneX, "it is appropriate" for the finding of intent to be based on a showing of "clear and convincing evidence." CAT3, LLC v. Black Lineage, Inc., 164 F. Supp. 3d 488, 498-99 (S.D.N.Y. 2016).

The burden of establishing the elements of a spoliation claim rests with the party seeking sanctions. Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 107 (2d Cir. 2002). A district court has "broad discretion" in deciding whether and how to sanction parties for spoliation of evidence. West, 167 F.3d at 779. "Even in the absence of a discovery order, a court may impose sanctions on a party for misconduct in discovery under its inherent power to manage its own affairs." Residential Funding Corp, 306 F.3d at 106-07. Additionally, "a finding of intent does not require a court to impose the sanctions listed under [37](e)(2)." Lokai Holdings, 2018 WL 1512055, at *8 (quoting Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment) (emphasis removed). Although dismissal of a lawsuit is within the court's discretion, it is a "drastic remedy" that "should be imposed only in extreme circumstances, usually after consideration of alternative, less drastic sanctions." West, 167 F.3d at 779 (quoting John B. Hull, Inc. v. Waterbury Petroleum Prods., Inc., 845 F.2d 1172, 1176 (2d Cir. 1988)) (internal quotation marks omitted).

B. Sanctions Are Warranted Under Rule 37(e)(2).[5]

1. Shipman's obligation to preserve ESI evidence.

The first element of the spoliation test requires that StoneX show that the lost ESI "should have been preserved in the anticipation or conduct of litigation" at the time it was

[5] Orders imposing discovery sanctions "are ordinarily considered non-dispositive, and therefore fall within the grant of Rule 72(a), 'unless the sanction employed disposes of a claim.'" Joint Stock Co. Channel One Russia Worldwide v. Infomir LLC, No. 16-CV-1318 (GBD) (BCM), 2017 WL 3671036, at *16 (S.D.N.Y. July 18, 2017) (quoting Seena Int'l Inc. v. One Step Up, Ltd., No. 15-CV-1095 (PKC) (BCM), 2016 WL 2865350, at *10 (S.D.N.Y. May 11, 2016)). StoneX seeks a case-dispositive sanction: the striking of Shipman's claims and the entry of default judgment against Shipman on StoneX's claims. Because I recommend that StoneX be awarded the relief it seeks, I do not have the authority to impose the requested sanction under

destroyed. Leidig v. Buzzfeed, Inc., No. 16-CV-542 (VM) (GWG), 2017 WL 6512353, at *8 (S.D.N.Y. Dec. 19, 2017) (citation and quotation marks omitted); Charlestown Cap. Advisors, 337 F.R.D. at 60-61. "A party's duty to preserve is based on a two-part inquiry: (1) when did the duty to preserve arise, and (2) what evidence was the party obligated to preserve?". Lokai Holdings, 2018 WL 1512055, at *9. "The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation."[6] Fujitsu Ltd. v. Fed. Exp. Corp., 247 F.3d 423, 436 (2d Cir. 2001); accord Resnik, 2019 WL 1434051, at *7 (quoting Rabenstein v. Sealift, Inc., 18 F. Supp. 3d 343, 360 (E.D.N.Y. 2014)). In a typical case, a party's duty to preserve relevant evidence is triggered no later than the date the action is commenced. Arista Records LLC v. Usenet.com, Inc., 608 F. Supp. 2d 409, 430 (S.D.N.Y. 2009). "[W]hen the duty to preserve evidence arises may, under certain circumstances, be dependent upon the nature of the evidence." Id.

Once a party is under a duty to preserve evidence pending litigation, it is not required to preserve "every document in its possession." Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003). That party, however, "is under a duty to preserve what it knows, or

Rule 72(a) and thus issue this report and recommendation. See Oracle USA, Inc. v. SAP AG, 264 F.R.D. 541, 546 (N.D. Cal. 2009) (explaining that magistrate judges lack authority to impose case-dispositive sanction and may only recommend the imposition of such a sanction).

[6] "The 2015 amendments to Rule 37(e) did not change previously existing federal standards concerning when a party's duty to preserve attaches and what evidence a party is obligated to preserve." Lokai Holdings, 2018 WL 1512055, at *9 n.8 (citing Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment); see also Charlestown Cap. Advisors, 337 F.R.D. at 61 ("The duty to preserve ESI imposed by Rule 37(e) incorporates th[e] longstanding common law duty.") (quoting Resnik v. Coulson, No. 17-CV-676 (PKC) (SMG), 2019 WL 1434051, at *7 (E.D.N.Y. Mar. 30, 2019)).

reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request." Arista Records, 608 F. Supp. 2d at 433 (quoting Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991)). "For the purposes of Rule 37(e), 'relevance' means relevance for purposes of discovery, which is an extremely broad concept." Cruz v. G-Star Inc., No. 17-CV-7685 (PGG), 2019 WL 4805765, at *11 (S.D.N.Y. Sept. 30, 2019) (internal quotations omitted) (quoting Orbit One Commc'ns, Inc. v. Numerex Corp., 271 F.R.D. 429, 436 (S.D.N.Y. 2010)).

This case commenced on January 24, 2023. See ECF No. 1. Although typically the duty to preserve evidence arises no later than the date an action is commenced, StoneX contends that Shipman's obligation to preserve ESI evidence arose earlier, on December 13, 2022. Pl.'s Br. at 4-5. By that date, StoneX's in-house counsel and Shipman's then-counsel had discussed potential claims by StoneX against Shipman, as well as potential claims by Shipman against StoneX following his termination. See ECF No. 108-3; see also Tr. at 20-23. Although the substance of those communications are unknown, it is apparent that Shipman had retained counsel and was contemplating litigation against StoneX. As such, the next question is whether Shipman should have known at that time that ESI in his possession may have been relevant to any contemplated future litigation.

Even if Shipman's contemplated litigation concerned only employment-related claims stemming from his termination on December 9, his obligation to preserve source code and StoneX's other proprietary and confidential information in his possession would still have arisen. Courts have "reject[ed] the notion that a party's obligation to preserve information arises only after it understands the *precise* nature of the *specific* litigation at issue." Pable v. Chicago Transit Auth., No. 19-CV-7868, 2023 WL 2333414, at *21 (N.D. Ill. Mar. 2, 2023) (alteration and italics in original). But even if the precise nature of Shipman's then-contemplated claims defined the scope of his duty to preserve, that duty would still have encompassed preservation of source code and other StoneX proprietary data. For example, StoneX's discovery that Shipman had retained Darwin source code, without authorization and following his termination, would have been after-acquired evidence that StoneX could have relied on to argue that it had lawful grounds for Shipman's termination and to limit his potential damages. See McKennon v. Nashville Banner Pub. Co., 513 U.S. 352, 361-62 (1995) (explaining that evidence that an employee would have suffered an adverse employment action for lawful reasons may limit the amount of damages a plaintiff may recover for termination).

In any case, even if a duty to preserve did not arise as of December 13, the duty certainly arose on December 27, 2022. See Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 73 (S.D.N.Y. 1991) (explaining that "the obligation to preserve evidence even arises prior to the filing of a complaint where a party is on notice that litigation is likely to be commenced.") On that date, outside counsel for StoneX sent a letter to Shipman's then-counsel, informing Shipman's counsel that StoneX was considering "filing claims against Mr. Shipman relating to and arising from his misappropriation of StoneX's confidential information and trade secrets." See ECF No. 108-4 at 1. The letter also indicated that counsel for Shipman had conveyed that Shipman has "various employment-related claims against StoneX." Id. Further, the letter instructed Shipman to specifically preserve "all copies in whatever form of the Project Darwin code, the Project Pascal [c]ode, or any code developed since the beginning of your Employment with StoneX." See id. at 2. And apart from the source code, the letter also listed various other types of ESI that Shipman was instructed to preserve. Id. at 1-2. Shipman admitted at oral argument that his attorney showed him the December 27 letter from StoneX. Tr. at 71-72. Thus, not only did the December 27 letter notify Shipman, himself, that StoneX was considering filing a lawsuit arising from Shipman's misappropriation of StoneX's confidential information, but the letter also expressly instructed Shipman to preserve StoneX confidential information, such as the source code, and his electronic devices, including laptop and desktop computers, USB drives, and the Linode cloud computers. See Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 436 (S.D.N.Y. 2004) ("[T]he duty to preserve and produce documents rests on the party. Once that duty is made clear to a party, either by court order or by instructions from counsel, that party is on notice of its obligations and acts at its own peril.").

Finally, even if the duty to preserve arose as late as January 24, 2023, when this suit commenced, Robinson's report indicates that Shipman deleted ESI evidence after that date. Specifically, CRA confirmed that Shipman on February 2, 2023, created a "script" that was used at least 79 times to execute the SDelete file wiping program on Shipman's desktop computer. Robinson Report ¶ 134.

2. *The destroyed ESI evidence cannot be restored or replaced through additional discovery.*

Under Rule 37(e), the party seeking sanctions must demonstrate that the alleged spoliated evidence was "lost." See Leidig, 2017 WL 6512353, at *7 ("[S]poliation sanctions can be imposed only when the party seeking such sanctions demonstrates that relevant evidence has been 'lost.'"); CBF Industria de Gusa S/A v. AMCI Holdings, Inc., No. 13-CV-2581 (PKC)

(JLC), 2021 WL 4190628, at *16 (S.D.N.Y. Aug. 18, 2021) (explaining that the moving party has the burden to show that lost ESI cannot be restored or replaced); see also Fed. R. Civ. P. 37(e) (requiring that ESI was "lost because a party failed to take reasonable steps to preserve it"). StoneX has met that burden here.

StoneX seeks sanctions for Shipman's spoliation of various types of ESI. See Pl's. Br. at 20. As it relates specifically to StoneX's source code files, CRA determined that 87 MB of data were transferred from a StoneX server computer (Corvo-004) on December 9, 2022; some of the files that were transferred contained Darwin source code; and the source code files were deleted that same day after they were transferred to a USB storage device. Robinson Report ¶¶ 14, 16, 78-87. In its complaint, StoneX alleged that it has been unable to locate a copy of the Darwin source code as it existed on December 9, 2022, the day Shipman presented a virtual presentation of the source code to the Quant Team at StoneX. Compl. ¶¶ 68-69; see also Declaration of Evan Pfeuffer, dated Jan. 18, 2023, filed under seal, ECF No. 2 ("Pfeuffer Decl.") ¶¶ 15-16. Additionally, CRA found evidence that source code files for Darwin and Texas existed on Shipman's StoneX laptop and were copied to a USB drive. But when CRA inspected the laptop, the source code files had been deleted and were not recoverable. And when Shipman turned over the USB drive to CRA for examination, the drive was not functional and the data on the drive had been destroyed. See Robinson Report ¶¶ 14, 16, 47-51, 118, 125, 158-61. What's more, CRA determined that 256 StoneX source code files were copied from Shipman's StoneX laptop and subsequently deleted. Robinson Report ¶¶ 40-43. In his deposition, Shipman admitted that the files contained the predecessor code to Darwin. See ECF No. 108-2 (573:5-574:5). The source code files were copied to a Sony USB drive which Shipman did not turn over despite his obligation to do so. Robinson Report ¶¶ 59, 175. CRA was unable to "locate any copies of the Darwin or other StoneX source code that Shipman accessed, copied, or deleted." Robinson Report ¶¶ 14, 16.

As another example, CRA found evidence that Shipman deleted, on December 14, 2022, a virtual computer and its storage drive that had previously existed on his StoneX laptop and which Shipman had used in the course of his employment with StoneX to develop source code. Robinson Report ¶¶ 52-55, 70, 119. In his deposition, Shipman admitted that he used the virtual computer to perform work for StoneX. See ECF No. 108-2 (594:5-18). CRA determined that the files contained on that virtual computer were not recoverable. Robinson Report ¶ 54. Shipman also "permanently destroyed" three Linode virtual computers, which CRA confirmed had been connected to StoneX computers. Robinson Report ¶¶ 89, 98, 101. Shipman also deleted the bash history log file from his StoneX laptop and that data too was not recoverable. Id. ¶¶ 64, 132. Likewise, Shipman deleted a virtual machine, deckard, from his StoneX laptop and CRA was unable to recover it. Id. ¶¶ 54-55. Additionally, all of the files that Shipman deleted through the use of file wiping programs like SDelete and Eraser were not recoverable and also prevented CRA from confirming whether the deleted data belonged to StoneX. Robinson Report ¶¶ 13-14, 17, 128-30, 134, 141.

Robinson's report details the extensive efforts by CRA to locate source code and other StoneX proprietary data on Shipman's various electronic devices. The report also explains how that lost ESI evidence cannot be entirely restored or replaced. In short, StoneX has amply shown that the ESI evidence has been lost and additional discovery would be fruitless.

3. *Shipman's failure to take reasonable steps to preserve ESI evidence and his intent to Deprive StoneX of that evidence.*

Under Rule 37, once the obligation to preserve relevant ESI attaches, a party in possession of that evidence must take "reasonable steps" to preserve it. Fed. R. Civ. P. 37(e). This requires the party to "suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." Lokai Holdings, 2018 WL 1512055, at *11 (quoting Treppel v. Biovail Corp., 249 F.R.D. 111, 118 (S.D.N.Y. 2008)); Doubleline Cap. LP v. Odebrecht Fin., Ltd., No. 17-CV-4576 (GHW) (BCM), 2021 WL 1191527, at *6 (S.D.N.Y. Mar. 30, 2021). "Where a party fails to timely institute 'a formal litigation hold and . . . otherwise informally preserve ESI,' the Court can conclude that it did not undertake reasonable steps to preserve ESI." Charlestown Cap. Advisors, 337 F.R.D. at 61 (quoting Capricorn Mgmt. Sys., Inc. v. Gov't. Employees Ins. Co., No. 15-CV-2926 (DRH) (SIL), 2019 WL 5694256, at *10 (E.D.N.Y. July 22, 2019)). "The 'reasonable steps' inquiry has been equated to 'roughly a negligent standard.'" Charlestown Cap. Advisors, 337 F.R.D. at 61 (quoting Leidig, 2017 WL 6512353, at *10). "Once the duty to preserve attaches, any destruction of documents is, at a minimum, negligent." Zubulake, 220 F.R.D. at 220.

To impose sanctions under subsection (e)(2), the court must determine that Shipman "acted with the intent to deprive another party of the information's use in the litigation." Fed. R. Civ. P. 37(e)(2). "The intent contemplated by Rule 37 is not merely the intent to perform an act that destroys ESI but rather the intent to actually deprive another party of evidence." Leidig, 2017 WL 6512353, at *11 (holding that although plaintiff intended to "disable his websites" and delete certain email files, he did not do so for the purpose of depriving defendants of the use of the ESI in litigation and therefore could not be sanctioned under subsection (e)(2)). "Courts in this Circuit have held that where a party has significantly failed in its obligation to preserve and collect documents, it is appropriate to infer intent to deprive." Fashion Exch. LLC v. Hybrid Promotions, LLC, No. 14-CV-1254 (SHS), 2021 WL 1172265, at *6 (S.D.N.Y. Mar. 29, 2021) (citing Ottoson v. SMBC Leasing & Fin. Corp., 268 F. Supp. 3d 570, 582-84 (S.D.N.Y. 2017)). "Other courts in this Circuit have inferred an 'intent to deprive' through circumstantial evidence where the data loss could not be 'credibly explained' other than by bad faith." CBF Industria de Gusa S/A, 2021 WL 4190628, at *18 (citing Moody v. CSX Transp., Inc., 271 F. Supp. 3d 410, 431 (W.D.N.Y. 2017)). In Moody v. CSX Transp., Inc., 271 F. Supp. 3d 410, 431 (W.D.N.Y. 2017), for example, the court looked at the following factors in assessing whether a party acted with the intent to deprive: "(1) evidence once existed that could fairly be supposed to have been material to the proof or defense of a claim at issue in the case; (2) the spoliating party engaged in an affirmative act causing the evidence to be lost; (3) the spoliating party did so while it knew or should have known of its duty to preserve the evidence; and (4) the affirmative act causing the loss cannot be credibly explained as not involving bad faith by the reason proffered by the spoliator."

I address the failure to preserve ESI together with the overwhelming evidence of Shipman's intent to deprive StoneX of that evidence because the two go hand in hand under the circumstances here. This is not a case where ESI was negligently or inadvertently lost. Nor is this a case where the intent to deprive must be inferred from circumstantial evidence. Robinson's report documents numerous instances where Shipman engaged in affirmative acts that resulted in the deletion and destruction of ESI, using software specifically designed for that purpose, leading

Robinson to conclude that in his 19 years conducting digital forensic investigations, he had "never encountered such a sustained and determined anti-forensic campaign" by one individual. Robinson Report ¶ 13.

The sheer scope of the spoliation engaged in by Shipman is unparalleled. Between December 13 and December 15, 2022, Shipman deleted three Linode computers on his account. Robinson Report ¶¶ 98-99, 101. On December 14, 2022, Shipman deleted sixteen folders containing StoneX confidential information and a virtual box (deckard), all of which had previously existed on his StoneX laptop. Id. ¶¶ 50-53. As Robinson explained, the deletion of the virtual box was equivalent to destroying an entire computer and its storage drive. Id. ¶ 54. On December 19, Shipman deleted folders containing StoneX source code on his StoneX laptop, at a time when the laptop's date and time had been altered and backdated. Id. ¶¶ 34, 42. Although CRA concluded that the source code files had been transferred to a SanDisk Cruzer USB drive prior to their deletion, the USB drive Shipman provided to CRA was nonfunctional and all of the data on it had been destroyed. Id. ¶ 158. On December 21, Shipman executed BitWipe and Eraser, two commercial file wiping programs that had to be downloaded from the Internet, to delete files on his desktop computer. Id. ¶¶ 61, 128-29. On December 22, Shipman deleted the bash history log file on his StoneX laptop, and that file contained a record of the historical events that had occurred on the laptop. Id. ¶¶ 64, 67. On December 26, Shipman downloaded and executed SDelete, another file wiping program, on his StoneX laptop. Id. ¶ 62. On February 2, 2023, Shipman created and used SDelete, another file wiping program,79 times on his personal desktop computer. Id. ¶ 134. Between February 2, 2023, and March 2, 2023, Shipman created and opened at least nine times a file that contained a "playbook" of anti-forensic information, an "xf" file, which he deleted on March 2. Id. ¶¶ 142-44. On March 2, the day CRA was scheduled to forensically image his computer, Shipman again executed SDelete on his desktop computer. Id. ¶ 130. Finally, the ShimCache and BAM on Shipman's desktop computer had no entries for the SDelete file wiping program, even though the program had been executed at least 94 times on the computer, suggesting that the entries had been deleted. Id. ¶¶ 142-46.

Robinson details numerous instances where Shipman took affirmative steps to permanently delete ESI evidence. Robinson also documents deliberate actions by Shipman to conceal his destruction of that evidence, such as the backdating of the date and time on his laptop computer, the deletion of the bash history logs, and the use of an anti-forensic playbook "xf" file. In short, there is clear and convincing evidence that Shipman affirmatively destroyed ESI and attempted to cover up its destruction, evincing an intent to deprive StoneX of that evidence.

Moreover, Shipman has offered no credible explanation for the loss of this ESI. For instance, CRA confirmed that on December 9, Shipman accessed the Corvo-004 StoneX server, transferred 87 MB of data, and deleted source code files and project folders, along with the bash history log. Robinson Report ¶¶ 70-87. In his January 27, 2023 declaration, Shipman stated that the Corvo-004 server was the "best candidate to retire," and it was "best practice" to "sanitize or remove sensitive data from servers before retirement." Shipman Decl. ¶¶ 15-17. Shipman further indicated that he ran "scripts or automated commands" to decommission the server, as he had done on dozens of occasions throughout the year. Id. ¶¶ 17-18, 31.

Shipman's explanation in his declaration did not comport with StoneX's practices or even with his own prior conduct. As Robinson stated, StoneX had not issued "any hard budgetary limitations" for the Microsoft Azure environment that hosted the Corvo-004 server, and the

Corvo-004 server was Shipman's primary development environment. Robinson Report ¶ 105. Robinson explained that it did not make sense for Shipman to have "decommissioned first" the Corvo-004 server "before the data could be transferred to another server" and "safely backed up." Id. Additionally, CRA found no evidence of any "server migration" scripts on the server or on Shipman's StoneX Laptop. Id. ¶ 106. Instead, CRA "identified deletion commands," which Shipman had used to "selectively delete[ ] individual files and folders," and "[t]he Corvo-004 Server itself was never "deleted or decommissioned." Id. According to Robinson, if Shipman had wanted to decommission the Corvo-004 server, he could have simply deleted the entire virtual computer.[7] Id.

Additionally, Shipman's false statements about his conduct further support a finding of bad faith. See Pable, 2023 WL 2333414, at *32 (finding intent to deprive sufficient for sanctions under Rule 37(e)(2) where spoliating party "fabricated" inconsistent accounts of what had transpired). For example, CRA's examination revealed that Shipman had used SDelete on his desktop computer 94 times between December 26, 2022, and March 2, 2023. Robinson Report ¶ 130. Yet, 21 days later, on March 23, 2023, Shipman testified during his deposition that he could not recall an instance of "downloading or running" SDelete on his desktop computer. See ECF No. 108-8 (187:5-10); see also id. (151:6-11). Then, in his June deposition, Shipman was asked if between December 9, 2022, and March 2023, he had "intentionally deleted materials"

[7] To be sure, any loss of ESI that occurred on December 9, 2022, would have predated Shipman's obligation to preserve that evidence. See supra Section B.1. Shipman, however, offered an implausible explanation for the transfer of 87 MB of data on December 9 and I note that because it further buttresses a finding of bad faith. In any event, Shipman provided inconsistent and contradictory statements about conduct he engaged in while under a duty to preserve evidence.

from his desktop computer, and Shipman testified that he did not recall using SDelete to remove the confidential health records of his children from his computer. See ECF No. 108-2 (427:8-12). Shipman further testified that he had "removed health records related to [his] children through conventional drag and drop to the trash bin." See id. (421:19-423:25). However, at oral argument on the instant motion, Shipman stated that he had used "SDelete to delete some personal family records to do with my children's mental health." Tr. at 46.

Even putting aside Shipman's shifting explanations for the use of SDelete and other commercial file wiping programs on his computer, the parties' joint forensic protocol expressly provided for the protection of the health records of Shipman's children. Thus, if Shipman's concern was that those health records not be examined by CRA, StoneX, or StoneX's counsel, the forensic protocol already afforded him that protection. Further, even if Shipman's explanation that he deleted confidential health records is credited, it does not explain why he testified during his June 2023 deposition that he deleted those records using "conventional drag and drop to the trash bin," but admitted at oral argument on the instant motion to using SDelete to delete those health records, despite testifying in his first deposition in March 2023 that he did not recall using SDelete and had not intentionally deleted materials.

Similarly, in his March deposition, Shipman testified that he could not "recall any situation where [he] deliberately tried to destroy evidence." See ECF No. 108-8 (181:5-11). He likewise testified that he had never run a "wiping program" on his StoneX laptop or personal desktop. Id. (151:6-23). Shipman's testimony was false, however. Between February and March 2023, Shipman used SDelete, a wiping program, 79 times. Robinson Report ¶ 134. Shipman also used other wiping programs, Eraser, and Bitwipe, on his personal desktop computer on

December 21, 2022. Id. ¶¶ 128-29. And, between December 13 and December 15, 2022, Shipman deleted three Linode computers from his account. Id. ¶¶ 98-99. During his deposition, Shipman also could not recall downloading the anti-forensic playbook file, "xf." See ECF No. 108-8 (190:23-191:20-22). But between February 2, 2023, and March 2, 2023, Shipman created and referenced the xf file nine times. Robinson Report ¶¶ 142-44.

Finally, this is not a case where the spoliated ESI evidence is unimportant or relevant to a peripheral issue in the litigation. The ESI evidence here is central to StoneX's claims. StoneX alleges that Shipman stole trade secrets and other proprietary and confidential information—namely, the source code for Projects Pascal and Darwin. And CRA's forensic examination revealed that Shipman deleted, and attempted to cover up his destruction of, that source code. Shipman thus destroyed the very thing he is accused of stealing. Additionally, because Shipman used wiping programs, failed to turn over USB drives, and deleted three Linode computers and the virtual box (deckard), it is impossible to determine whether Shipman also destroyed other information that would have been helpful to StoneX in prosecuting its claims or defending against Shipman's claims.

In sum, StoneX has shown that Shipman failed to take reasonable steps to preserve ESI he was under a duty to preserve and did so to intentionally deprive StoneX of that evidence.

4. Terminating sanctions are the appropriate remedy.

Determining an "appropriate sanction lies within the sound discretion of the trial court." Arista Records LLC, 633 F. Supp. 2d at 141. Even where there is "strong evidence of extreme wrongdoing, courts must be wary of issuing case-dispositive sanctions; such sanctions 'should be imposed only in extreme circumstances, usually after consideration of alternative, less drastic sanctions.'" Id. (quoting West, 167 F.3d at 779). StoneX has met its burden of establishing the elements for imposition of sanctions under Rule 37(e)(2). What's more, this is the extreme circumstance where anything less than a case-dispositive sanction would not be appropriate.

Shipman's conduct here is as far from the inadvertent, negligent, or even reckless loss of ESI evidence as could exist. Shipman engaged in a months-long campaign to intentionally spoliate multiple categories of ESI. Because of the broad scope of the spoliation, the precise contents of the destroyed files cannot be determined. Moreover, Shipman has repeatedly lied in connection with his spoliation of that ESI, including under oath during two depositions. He has fabricated implausible and contradictory explanations for his conduct. See Pable, 2023 WL 2333414, at *34 (reasoning that terminating sanctions where appropriate, in part, because spoliating party "lied repeatedly" in connection with the spoliation).

An adverse-inference instruction would not be an adequate remedy because of the wide-ranging scope of the spoliation. The Court cannot ascertain precisely what information was destroyed by Shipman and what issues or claims that data was relevant to, and thus "there is no way to approximate the presumably unfavorable effect of that information" for purposes of attempting to craft a jury instruction or adverse inference that would mitigate or cure the prejudice to StoneX. Williams v. Am. College of Edu., Inc., No. 16-C-11746, 2019 WL 4412801, at *16 (N.D. Ill. Sept. 16, 2019); see also Pable, 2023 WL 2333414, at *35 (explaining that no lesser sanction would be sufficient to address the prejudice to defendant where scope of spoliation made it impossible to determine the specific content of the spoliated evidence). Shipman's intentional spoliation of the source code has "obfuscated the true merits" of StoneX's claims and made it impossible for StoneX to gather the information it needs to prove its claims, such that a resolution on the merits, although generally preferable, is "no longer a viable option." Williams, 2019 WL 4412801, at *16. Additionally, the Court cannot determine whether Shipman also destroyed evidence that would have been favorable to StoneX in defending against Shipman's counterclaims. See Leon v. IDX Sys. Corp., 464 F.3d 951, 960-61 (9th Cir. 2006) (affirming dismissal as a spoliation sanction where "any number of the [deleted] files could have been relevant to [the defendant's] claims or defenses" and it was "impossible to identify which files and how they might have been used"). Under these circumstances, a lesser sanction would not address the "severity of the data destruction" that has occurred here. TLS Mgmt. & Marketing Servs., LLC v. Mardis Fin. Servs, Inc., No. 14-CV-881 (CWR) (LRA), 2018 WL 3673090, at 7 (S.D. Miss. Jan. 29, 2018); see also Balancecxi, Inc. v. Int'l Consulting, No. 19-CV-0767, 2020 WL 6886258, at *14 (W.D. Tex. Nov. 24, 2020) (imposing terminating sanctions under Rule 37(e)(2) where defendants "deleted evidence multiple times, did so intentionally, and did so despite knowing they had a duty to preserve evidence").

Finally, Shipman's spoliation required StoneX to incur unnecessary attorneys' fees in bringing the instant motion. A "consideration in choosing an appropriate sanction" is to "restore" Plaintiffs to the position they would have been in had Shipman "faithfully discharged [his] discovery obligations." Zubulake, 229 F.R.D. at 437. Plaintiffs retained CRA even before the suit was filed, and it is not apparent that Plaintiffs could have proven their claims without a forensic examination of Shipman's electronic devices. Thus, even without Shipman's spoliation, it appears that Plaintiffs would have incurred the expert costs related to CRA. However, Shipman's spoliation required Plaintiffs to expend unnecessary attorneys' fees in filing the instant motion. I thus recommend that StoneX be awarded its attorneys' fees and costs incurred in filing the spoliation motion. See id. (awarding adverse inference instruction and costs of spoliation motion); see also Richard Green (Fine Paintings) v. McClendon, 262 F.R.D. 284, 292 (S.D.N.Y. 2009) ("Monetary sanctions are appropriate to punish the offending party for its actions [and] to deter the litigant's conduct, sending the message that egregious conduct will not be tolerated.") (internal quotation marks and citations omitted; alteration in original); Pable, 2023 WL 2333414, at *36-37 (recommending award of terminating sanctions and attorneys' fees and costs incurred in bringing the spoliation motion).

CONCLUSION

For the foregoing reasons, I respectfully recommend that Plaintiffs' motion for sanctions be **GRANTED**. I thus recommend that Defendant's cross claims be stricken, default judgment be entered against Defendant, and Plaintiffs be awarded their attorneys' fees and costs for the instant motion.

DATED: New York, New York
February 5, 2024

Respectfully submitted,

VALERIE FIGUEREDO
United States Magistrate Judge

PROCEDURE FOR FILING OBJECTIONS TO THIS REPORT AND RECOMMENDATION

Pursuant to 28 U.S.C. § 636(b)(1) and Rule 72(b) of the Federal Rules of Civil Procedure, the parties have fourteen (14) days (including weekends and holidays) from service of this Report and Recommendation to file any objections. See also Fed. R. Civ. P. 6(a), 6(b), 6(d). A party may respond to any objections within 14 days after being served. Any objections and responses shall be filed with the Clerk of the Court. Any request for an extension of time to file objections or responses must be directed to the Honorable John G. Koeltl. If a party fails to file timely objections, that party will not be permitted to raise any objections to this Report and Recommendation on appeal. See 28 U.S.C. § 636(b)(1); Fed. R. Civ. P. 72; Fed. R. Civ. P. 6(a), 6(b), 6(d); Thomas v. Arn, 474 U.S. 140 (1985); Wagner & Wagner, LLP v. Atkinson, Haskins, Nellis, Brittingham, Gladd & Carwile, P.C., 596 F.3d 84, 92 (2d Cir. 2010).